Appendix G: Use/Disclosure of PHI in Daily Work- A Quick Reference Guide

FSSA/OMPP staff members will use and disclose PHI in their daily work activities, within the authorized, routine duties of their assigned positions.

For example, if an IHCP member calls staff member X to obtain his or her PHI, staff member X may disclose the requested protected health information ONLY AFTER staff member X follows proper protocols to confirm the identity and authority of the member.

It is the obligation of each FSSA/OMPP staff member to follow proper protocols whenever PHI is used or disclosed.

Specific information regarding requirements and procedures for the use and disclosure of a member's PHI is contained throughout this manual, in the appropriate sections. FSSA/OMPP staff members must become familiar with these processes and should utilize the complete manual as an ongoing resource.

This appendix is provided as a "quick reference guide", which integrates pertinent protocols to be used by FSSA/OMPP staff members specifically for instances when an individual requests a member's PHI (including when the member requests their own PHI) from a FSSA/OMPP staff member and for FSSA/OMPP staff member's daily use and access to a member's PHI in the course of their authorized, routine duties.

Phone Requests for Disclosure of PHI

FSSA/OMPP staff members must be aware that the *Privacy Rule* requires that certain rules be followed regarding the PHI that can be disclosed to the caller, the situations in which PHI can be directly disclosed, and the situations when no PHI can be disclosed to the caller. The following procedures are to be followed by FSSA/OMPP staff members prior to releasing any PHI pursuant to a phone call. A flowchart, the FSSA/OMPP Member Phone Request Work Flow, is also provided to outline the process to be followed (see Figure G.1 in this appendix).

Phone Call Scenarios:

The member, or the parent of a member who is under the age of 18, calls FSSA/OMPP staff member to request program eligibility, benefit, benefit limitation, or specific service billing (claim) information.

Follow these procedures:

Request program eligibility, benefit, benefit limitation, or specific service billing (claim) information.

Ask the caller for all of the following information to confirm the identity and authority of the caller, and use the information on the Indiana*AIM* Recipient subsystem (under the member's RID number) to confirm if the information is correct:

- Member name; and
- Member address; and
- Member RID number; and
- Member Social Security Number or member birth date.

If the caller is the member's parent, verify parental information on Indiana*AIM* (e.g. mother has name and RID number under *Recipient Mother RID* window).

If the information is **not consistent** with the information as noted in Indiana*AIM*, do not disclose the requested information. If the caller provides an address that is not in Indiana*AIM*, refer the member, or the member's parent, to the caseworker for an update to the ICES. PHI cannot be released until the information in Indiana*AIM* is consistent with the information provided by the caller.

If the caller provides the information as noted in Indiana*AIM,* ask the caller what specific information is requested. If the request is for program eligibility, benefit, benefit limitation, or service billing information (do not provide diagnosis), provide the information.

If the caller requests the information in writing (rather than over the phone), refer the member to the IHCP Privacy Office so that the request may be documented on the *Member Request for Information* form. The completed form will be submitted to the IHCP Privacy Office for response.

The member's adult child or relative, who is not the legal guardian or personal representative of the member, calls an FSSA/OMPP staff member to request program eligibility, benefit, or benefit limitation regarding the member.

Follow these procedures:

Request program eligibility, benefit, or benefit limitation regarding the member.

Provide limited information after verbal verification of the caller and member's identity. Information that may be provided in response to a phone inquiry is limited to:

- Program eligibility information
- Coverage or benefit limitation information
- Basic billing information, e.g., claim payment.

Do not provide information diagnosis or procedure codes or any specific information over the phone.

Tell the caller that **the member** must submit a written authorization form (refer to the IHCP Privacy Office). The IHCP Member Authorization form must be submitted to the Privacy Office.

The member's legal guardian or personal representative calls an FSSA/OMPP staff member to request program eligibility, benefit, or benefit limitation regarding the member.

Follow these procedures:

Request program eligibility, benefit, or benefit limitation regarding the member.

Provide limited information after verbal verification of the caller and member's identity. Information that may be provided in response to a phone inquiry is limited to:

- Program eligibility information
- Coverage or benefit limitation information
- Basic billing information, e.g., claim payment.

Do not provide information diagnosis or procedure codes or any specific information over the phone. Refer the requestor to the IHCP Privacy Office.

Proof of identity and proof of authority must be submitted to the IHCP Privacy Office prior to release of information (the *Verification of Identity and Authority* form will be used for this).

The Member's IHCP health care provider calls an FSSA/OMPP staff member to request information about the member.

Information regarding the member's treatment may be shared with the member's provider. Payment or health care operation discussions must be limited to the minimum necessary to answer the provider's question.

The Member's Attorney calls an FSSA/OMPP staff member to request information about the member.

No information will be disclosed to a member's attorney. Specific requests regarding third party liability (TPL) should be referred to the EDS TPL Unit. All other requests must be submitted in writing to the IHCP Privacy Office.

Worker's Compensation Request

No information will be disclosed to Worker's Compensation by an FSSA/OMPP staff member. Specific requests regarding Worker's Compensation should be referred to the EDS TPL Unit.

Legislative Request

Written requests may include a signed and authorized HIPAA compliant form or an Authorization to Act on Behalf of Constituent Form, or written correspondence or e-mail received from the constituent which includes verifiable personal information (such as social security number, case number and/or date of birth) and which clearly authorizes a Legislative staff member to receive the confidential information. In the absence of a written request, personal knowledge of the constituent's agreement to the release of the confidential information through participation in a meeting or conference call, which includes the constituent and a member of the agency's legislative team, may be sufficient.

DISCLOSING PHI: Written Requests

All written requests for PHI access should be submitted to the IHCP Privacy Office for processing. If an FSSA/OMPP staff member receives a written request, the staff member must forward the request to the IHCP Privacy Office promptly.

Requests related to TPL will continue to be handled by the EDS TPL Unit.

Your Access to PHI

Use of PHI in your job

As an FSSA/OMPP staff member, you have access to IHCP member PHI. Your appropriate unit supervisor is responsible for ensuring that you only have access to the minimum amount of PHI needed to perform your job duties.

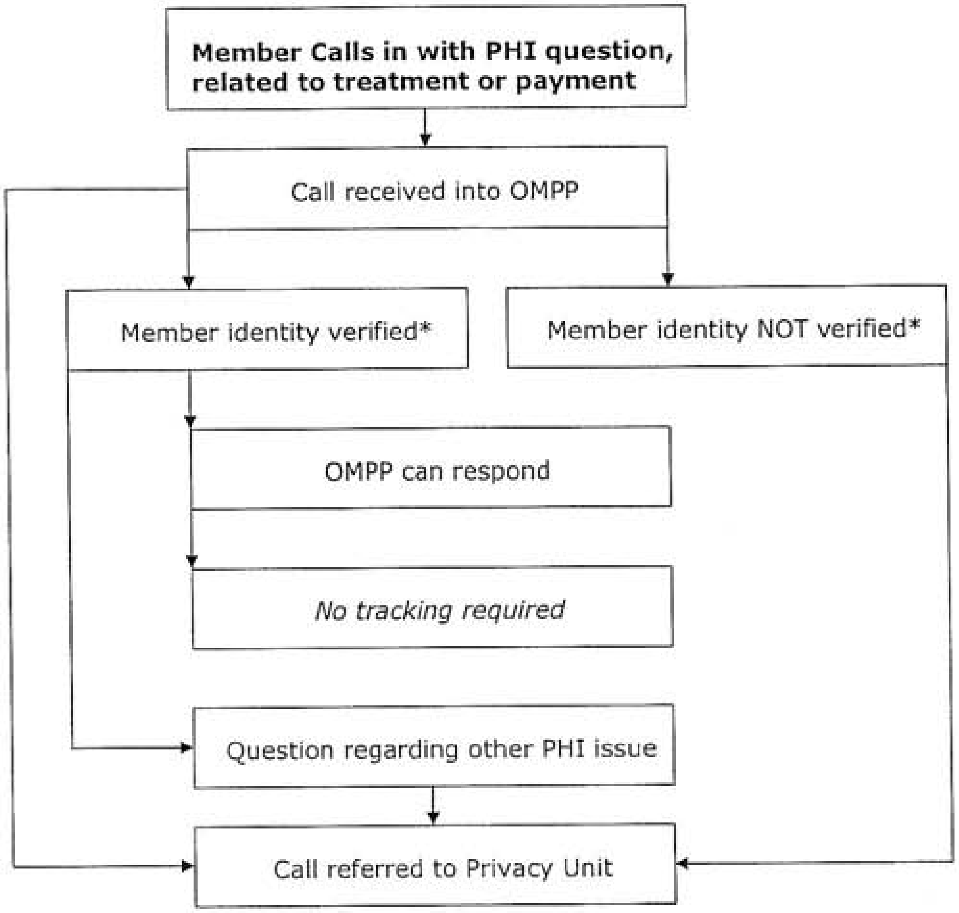
It is your responsibility to be familiar with the contents of this manual, and to provide protection and security to all PHI that you have access to, including PHI access through the IHCP office in addition to off-site access.

Please be aware that IHCP members' PHI may be in written, electronic, or oral forms. All forms must be protected from any inappropriate use or disclosure, as required by the *Privacy Rule*.

Workstation Requirements

FSSA/OMPP staff members are responsible for maintaining a secure personal working environment. Please carefully review Section 20 of this manual, *Protected Health Information Safeguards*, to ensure that you are adequately protecting IHCP members' PHI.

Figure G.1: Member Phone Request Work Flow


Member Calls in with PHI question, related to treatment or payment
Call received into OMPP
Member identity verified*
Member identity NOT verified*
OMPP can respond
No tracking required
Question regarding other PHI issue
Call referred to Privacy Unit

* Use Protected Health Information (PHI) Inquiry Grid

Table G.1: Protected Health Information (PHI) Inquiry Grid

Person/Entity Requesting PHI	**PHI is for a member(s) who is:**		
	Age 18 or older, or an emancipated minor (note 1)	**Under Age 18**	**Age 18 or older and has a legal guardian or personal representative**
Member	No restriction after verbal or written verification of member identity (note 2)	N/A	No restriction after verbal or written verification of member identity (note 2)
Member's Parent	No disclosure without written authorization from the member (note 3)	No restriction after verbal or written verification of member identity and parent identity (note 2, and verify parental information if possible)	Provide limited information after verbal verification (note 4); No restriction after written verification of member and parent identity and authority, if parent is guardian or representative (note 5)
Member's legal guardian or personal representative	Provide limited information after verbal verification (note 4); No restriction after written verification of guardian/ representative identity and authority (note 5)	Provide limited information after verbal verification (note 4); No restriction after written verification of guardian/ representative identity and authority (note 5)	Provide limited information after verbal verification (note 4); No restriction after written verification of guardian or personal representative identity and authority (note 5)
Member's adult child	Provide limited information after verbal verification (note 4); No restriction after written authorization from the member (Note 3)	N/A	Provide limited information after verbal verification (note 4); No restriction after written authorization from the member (Note 3)
Member's significant other	Provide limited information after verbal verification (note 4); No restriction after written authorization from the member (Note 3)	N/A	Provide limited information after verbal verification (note 4); No restriction after written authorization from the member (Note 3)
Member's IHCP health care provider	No restriction on TPO-related discussions (note 6)	No restriction on TPO-related discussions (note 6)	No restriction on TPO-related discussions (note 6)
Attorney	No disclosure without written authorization from the member (note 3)	No disclosure without written authorization from the member (note 3)	No disclosure without written authorization from the member (note 3)
Legislative Staff	No disclosure without written authorization from member; or without direct request from member via a meeting or conference call. (note 7)	No disclosure without written authorization from member; or without direct request from member via a meeting or conference call. (note 7)	No disclosure without written authorization from member; or without direct request from member via a meeting or conference call. (note 7)
Worker's Compensation (note 8)	No restriction on TPO-related discussions (note 8)	No restriction on TPO-related discussions (note 8)	No restriction on TPO-related discussions (note 8)

Continued... Protected Health Information (PHI) Inquiry Grid

Table G.1 NOTES:

1: Written verification of minor's emancipation is required.

2: Member must provide name, address, RID number, and either the social security number or birth date. Verify all information to member information on Indiana*AIM*. If the information does not match, do not disclose information. If member has new address, refer member to caseworker who will make change to ICES. Member can call back after new address is on Indiana*AIM*.

3: The member must submit a written authorization form to the IHCP Privacy Office prior to disclosing the PHI.

4: Follow member identity process in Note 2, and if possible, verify parental information on IndianaAIM (e.g., mother has name and RID number under *Recipient Mother RID* window).

Provide only the following information in response to a phone inquiry:

- Program eligibility information
- Coverage or benefit limitation information
- Basic billing information, e.g., claim payment

Do **NOT** provide diagnosis or procedure codes or any specific information over the phone.

5: The legal guardian or personal representative must submit proof of identity and proof of authority to the IHCP Privacy Office prior to disclosure (e.g., completion of the *Verification of Identity and Authority* form, and documentation supporting authority to act on behalf of member). Refer caller to the IHCP Privacy Office to obtain this form.

6: Information regarding the member's treatment can be shared with the provider without the minimum necessary requirement. All other payment or health care operation discussions must be limited to the minimum necessary to answer the question.

7: Written requests may include a signed and authorized HIPAA compliant form or an Authorization to Act on Behalf of Constituent Form, or written correspondence or e-mail received from the constituent which includes verifiable personal information (such as social security number, case number and/or date of birth) and which clearly authorizes a Legislative staff member to receive the confidential information. In the absence of a written request, personal knowledge of the constituent's agreement to the release of the confidential information through participation in a meeting or conference call, which includes the constituent and a member of the agency's legislative team, may be sufficient.

8: The EDS TPL Unit will handle all Worker's Compensation cases.

Table G.2: Protected Health Information Authorization Requirements

PHI release requested to/for:	Authorization Required *(from member)*	Tracking Required	Minimum Necessary Standard
To a member	No	No	No- after verification of identity,
To a member's personal representative/legal guardian *Limited information may be disclosed by OMPP, however, the IHCP Privacy Office must have written verification of the legal guardian or personal representative's identity and authority prior to disclosing more specific information (refer to Table G.1).*	No	No	No- after verification of identity,
To a member's health care provider*	No	No	No- after verification of identity,
To a member's attorney	Yes	No	No- after authorization,
To a member's legislative representative	Yes	No	No- after authorization,
To a deceased member's personal representative *Limited information may be disclosed by OMPP, however, the IHCP Privacy Office must have written verification of the legal guardian or personal representative's identity and authority prior to disclosing more specific information (refer to Table G.1).*	No	No	No- after verification of identity,
For payment purposes*	No	No	Yes
For health care operation purposes*	No	No	Yes
Required by law	No	The tracking requirement for law enforcement purposes is dependent upon the member's status and the nature of the	PHI released must be limited to the relevant requirements of the specific law.

Deleted: No

Deleted: No

Deleted: No

Deleted: No

Deleted: No

Deleted: No

PHI release requested to/for:	Authorization Required *(from member)*	Tracking Required	Minimum Necessary Standard
		disclosure.	
For public health activities	No	Yes	PHI released must be limited to the relevant requirements of the specific law.
For law enforcement purposes	No	Yes	Yes
For health oversight activities	No	Yes-The tracking may be temporarily suspended when requested by the health oversight agency or official.	Yes
For worker's compensation activities	No	Yes	Yes
To the Secretary of HHS	No	Yes	No
De-identified information	No	No	Individually identifiable information is removed before disclosure.
Limited data set *Limited data set requests and disclosures may only be used for research, public health, or health care operation purposes.*	No	No	Select direct identifiers are removed from information before disclosure.
By a whistleblower	No	No	Yes
By a workforce crime victim	No	No	Limited to the requirements in 45 CFR 164.502(j)
Prior to April 14, 2003	N/A	No	No

* Psychotherapy notes can be disclosed without member authorization ONLY for the following specific treatment, payment, and health care operations:

- Use by the originator of the psychotherapy notes for treatment
- Use or disclosure by the IHCP to defend itself in a legal action or proceeding brought by the member
- A use or disclosure permitted with respect to the oversight of the health care provider originating the psychotherapy notes.
- For any other use, coordinate with the OMPP Privacy Coordinator.

Appendix H: Requests to Legislative Staff

Note: This is not an official form. For an official form, please contact the IHCP Privacy Office.

I request and authorize Rep/ Sen.__________________ (or a staff member designated by the legislator) to place an inquiry on my behalf and to receive confidential information from the proper officials regarding my concern. I realize this may involve the disclosure of confidential information, including but not limited to health information otherwise protected as confidential under the Health Insurance Portability and Accountability Act (HIPAA). I hereby grant permission to Rep. /Sen. ___________________ (or designated staff member) to receive this information in order to address my concerns.

I authorize only the release of information directly relevant to my inquiry.

This authorization shall automatically expire within sixty (60) days of date of the form, unless written notice of revocation is received by Sen./ Rep. ___________prior to that date.

Constituent Name: ____

Name of Individual Subject of Inquiry (if other than the Constituent)__________________

Relationship to Constituent:____

Constituent / Subject
Address:____

Constituent Signature:__________________________________ Date: __________

Description of the situation/inquiry:

____

____

____

____

____

____

____

Note: Federal privacy regulations require your authorization in order for our office to receive confidential health information from certain agencies.

Appendix I: Personal Representative Authorization Form

Please click on the following link to access the Personal Representative Authorization Form:

Form SF51732

Appendix J: Member Restriction Request Form

Please click on the following link to access the Member Restriction Request Form:

Form SF51740

Appendix K: Member Accounting Request Form

Please click on the following link to access the Member Accounting of Disclosures Request Form:

Form 51738

ATTACHMENT C.

FORM A-1 REQUEST FOR BULK DATA/ COMPILED INFORMATION

Family and Social Services Administration

Office of Medicaid Policy and Planning

HIPAA Security Policy and Procedure Manual

VERSION 8.0 *(April 25, 2007)*

Deleted: 7.02

Deleted: *10*

Table of Contents

Deleted: 1-2
Inserted: 1-2
Deleted: 1-2
Deleted: 1-6
Inserted: 1-6
Deleted: 1-6
Deleted: 1-6
Inserted: 1-6
Deleted: 1-6

Deleted: 7-2
Inserted: 7-2
Deleted: 7-2

Deleted: 8-2
Inserted: 8-2
Deleted: 8-2

HIPAA

The *Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191*, was enacted on August 21, 1996. HIPAA contains three major provisions:

- Portability – Final rule published in 1997;
- Fraud and abuse/Medicare integrity program – Final rule published in 1998; and
- Administrative simplification – First final rule published August 17, 2000.

Administrative Simplification

The purpose of the administrative simplification provision is to improve health programs and the effectiveness and efficiency of the health care industry. This is accomplished by adopting common standards for health plans, health care clearinghouses, and health care providers that transmit or store any of the covered transactions provided in the *Standards for Electronic Transactions* final rule. As a health plan, the IHCP is required to comply with all HIPAA-related rules pertaining to:

- Administrative transactions,
- Unique identifiers,
- Code sets,
- Privacy, and
- Security.

Security

The Indiana Health Coverage Programs (IHCP) includes the Family and Social Services Administration (FSSA), Office of Medicaid Policy and Planning (OMPP). For the purposes of the Health Insurance Portability and Accountability Act (HIPAA) Standards for Security final rule, as published February 20, 2003, the OMPP has been designated as a health care component of FSSA (i.e., the covered entity).

Deleted: 7.02

Deleted: 10

As a covered entity, OMPP is required to comply with all requirements in the *Security Rule,* and required to ensure that other

Security *(cont.)*

components of the hybrid entity (FSSA) do not have access to electronic PHI unless such access is necessary for program administration, and those components agree to abide by the *Security Rule*. OMPP must have written policies, procedures, and safeguards in place, and all OMPP staff must be trained on these requirements, by April 20, 2005.

The Department of Administration and the Department of Information Technology's Division of Technology Services will maintain responsibility for overall facility security, including but not limited to the security of lines into and out of the facility, and network security. OMPP will implement additional controls, beyond FSSA controls, as specified in this manual and as necessary to ensure for optimal protection of electronic PHI.

Business associates will also be required to comply with the *Security Rule* for the functions contracted by OMPP. This manual provides policies and procedures that OMPP must comply with, including a requirement to maintain Business Associate Agreements to ensure appropriate compliance from business associates as applicable. Business associate provisions are incorporated into OMPP's standard contractual language. For a complete definition of business associate, refer to the ***Section 15: Glossary*** included in this manual.

Formatted: Font: 12 pt, Bold, Italic

Deleted: *Section 15: Glossary*

The Department of Health and Human Services (HHS), has determined that the Centers for Medicare and Medicaid Services (CMS) will be the enforcing agency for the *Security Rule*. Hereafter, the Secretary of the HHS will be referred to as the Secretary.

Overview

The *Family and Social Services Administration (FSSA), Office of Medicaid Policy and Planning (OMPP), HIPAA Security Policy and Procedure Manual* is designed to provide the OMPP staff member with the policies and procedures necessary to comply with the *Health Insurance Portability and Accountability Act (HIPAA) Standards for Security* final rule, published February 20, 2003.

Note: OMPP is designated as a health care component of FSSA. As a health care component of FSSA, OMPP must not disclose protected electronic health information to another component of FSSA unless the other component of FSSA agrees to follow the applicable Security provisions contained within a Memorandum of Understanding (MOU), and such disclosure is the minimum necessary for program administration.

FSSA AD1-18

Deleted: *7 02*

Deleted: *10*

FSSA Policy # AD1-18 requires all FSSA divisions to adhere to relevant HIPAA policies regarding the use or disclosure of PHI.

Security Regulations

The Standards can be found in *45 Code of Federal Regulations* (CFR) *Parts 160, 162 and 164*. Hereafter, the Standards will be known as the *Security Rule.*

The FSSA has an established Security Office.

Administration of Security Regulations

Kathee Saylor
FSSA Security Manager
Office of Systems Development and Support
Division of Technology Services
Mail Stop 17, P.O. Box 7083
Indianapolis, IN 46207-7083

The phone number for the FSSA Security Office is: (317) 232-1263.

The FSSA Security Office point of contact for the OMPP staff is the OMPP Security Coordinator. OMPP designated a qualified member of OMPP, possessing appropriate experience, as the OMPP Security Coordinator. The OMPP Security Coordinator will be responsible for ensuring that OMPP staff members and contractors are in compliance with the *Security Rule.* Any questions regarding the *Security Rule* should be directed to the OMPP Security Coordinator. The current OMPP Security Coordinator is Jenifer Nelson, and can be reached at (317) 232-4305. Jenifer Nelson also serves as OMPP's Privacy Coordinator. Documentation regarding these designations shall be maintained for six years.

The FSSA Security Office and the OMPP Security Coordinator, along with all members of the OMPP staff, are responsible for the overall compliance with the HIPAA rules and regulations relating to security of electronic health information. This includes Medicaid and all associated programs, the Children's Health Insurance Programs (CHIP), and 590 Program.

Deleted: *7.02*

Deleted: *10*

HIPAA Compliance: Role of OMPP Staff Members

OMPP staff members will continue to use electronic protected health information within the authorized, routine duties of their assigned positions. Staff members must be cognizant of the *Security Rule* in carrying out these authorized duties. This manual details procedures that each staff member must follow when using electronic PHI.

OMPP staff members must be fully aware of all requirements contained within the *Security Rule* in carrying out their authorized duties. This manual details procedures that each OMPP staff member must be aware of and follow to ensure the security of all electronic health information.

Any questions that OMPP staff members may have regarding the *Security Rule* should be directed to the OMPP Security Coordinator.

NOTE: The policies and procedures contained within this *HIPAA* ***Security*** *Policy and Procedure Manual* supplement information provided in the *HIPAA* ***Privacy*** *Policy and Procedure Manual*, and therefore should be used in conjunction with the *HIPAA* ***Privacy*** *Policy and Procedure Manual.*

Requirements of the IHCP

OMPP, as a designated covered entity, must ensure the provision of adequate protection and security to a member's electronic protected health information (PHI) that is transmitted or maintained electronic form, to safeguard electronic PHI from unauthorized access, alteration, deletion, and transmission.

In general, the Indiana Health Coverage Programs (IHCP) must do the following to ensure compliance with HIPAA Security standards:

- Designate the health care component of the organization and determine associated organizational requirements. OMPP has been designated as a health care component of the hybrid entity, FSSA.
- Ensure the confidentiality, integrity, and availability of all electronic protected health information that is created, received, maintained or transmitted by the health care component.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures

Deleted: *7.02*

Deleted: *10*

of such information that are not permitted or required by this subpart.

- Ensure compliance with this subpart by its workforce.

Distinctions between the Security Rule and Privacy Rule

Security and Privacy are inextricably linked. However, there are distinct differences between the *Privacy Rule* and the *Security Rule*. The *Privacy Rule* addresses protection and security of PHI in any form, including oral communication; whereas the *Security Rule* is more limited as it applies specifically to protections and security of electronic PHI. OMPP staff should refer to the *HIPAA Privacy Policy and Procedure Manual* for specific instruction on how protected health information should be controlled through requirements relating to authorized uses and disclosures, and rights of patients to access their health information.

What is Protected Health Information (PHI)?

A member's PHI includes, but is not limited to, the demographic information, recipient identification number (RID) number, and claim information (accounting or claim payment). For a complete definition of *protected health information*, refer to ***Section 15: Glossary***, included in this manual.

Formatted: Font: 12 pt, Bold, Italic

Deleted: *Section 15: Glossary*

Use of PHI in daily work activities

The *Security Rule* requires each OMPP staff member to be aware of the electronic PHI that they use in their daily work activities. Staff members are responsible for protecting electronic PHI in their work functions and work environment.

The *Security Rule* includes administrative, physical, and technical safeguard requirements to ensure the confidentiality, integrity, and availability of all electronic protected health information OMPP creates, receives, maintains or transmits, and to protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

> **NOTE: The policies and procedures contained within this manual are not intended to prevent staff members from using and disclosing electronic PHI within the authorized, routine duties of their assigned positions. The procedures OMPP staff must follow when carrying**

Deleted: *7.02*

Deleted: *10*

out these authorized duties are detailed throughout the appropriate sections of this manual, and are further examined in the *HIPAA Privacy Policy and Procedure Manual*.

Document Organization

This manual contains the following information for the employee's reference and use regarding security of electronic health information.

- Security policy and procedure sections, containing:
  - The purpose of the section,
  - The OMPP-specific policy, and
  - The OMPP-specific procedure.
- Glossary explaining terms in relation to the HIPAA *Security Rule*.
- Appendix A, providing a crosswalk of Security Rule implementation specifications, as detailed in the *HIPAA Security Rule Initial Assessment*, to policies and procedures contained within this manual.
- Appendices B through D containing forms referenced in this manual.

Note: Where appropriate, Code of Federal Regulations (CFR) citation(s) are provided. For additional information regarding the policy and procedures, refer to the CFR.

Definitions

For a complete listing of definitions associated with the *Security Rule*, refer to the ***Section 15: Glossary***.

Formatted: Font: 12 pt, Bold, Italic

Deleted: *Section 15: Glossary*

Summary

HIPAA rules and regulations

On August 21, 1996, the Health Insurance Portability and Accountability Act, commonly known as HIPAA, was signed into law. As its name implies, HIPAA included a number of provisions to make health coverage more portable for employees changing jobs by limiting exclusions for pre-existing conditions. In addition, HIPAA also included a set of "Administrative Simplification" provisions, which were intended to improve the efficiency and effectiveness of the health care system.

Deleted: 7.02

Deleted: 10

In drafting HIPAA, Congress recognized the threats to confidentiality posed by the growing complexity of the health care system and the increased used of electronic data interchange that HIPAA itself was intended to encourage. Thus, the Administrative Simplification provisions of HIPAA authorized the U.S. Department of Health and Human Services (HHS) to issue standards for the security of electronic health information. On August 12, 1998, HHS published proposed regulations to establish minimum standards for security of electronic health information. The Department reviewed more than 2,300 comments in response to the proposed rule and published a final rule on February 20, 2003.

Purpose of this manual

This manual is a resource provided to assist OMPP staff members in interpreting the *Security Rule*. Key components of the *Security Rule* are presented in sections. Policies and procedures, specific to OMPP, are provided in each section.

It is important for all OMPP staff to be knowledgeable of the *Security Rule*, as presented in this manual, in addition to the policies and procedures specific to the IHCP. This manual is to be used in conjunction with the *HIPAA Privacy Policy and Procedure Manual*, to ensure full compliance with HIPAA rules and regulations.

Questions or concerns relating to security

The role and responsibilities of the OMPP Security Coordinator are detailed in the attached file.

Responsibilities

Any questions that OMPP staff may have regarding the contents of this manual, or questions relating to security, will be directed to the OMPP Security Coordinator.

If you have any concerns or doubts about the security of any electronic PHI, contact the OMPP Security Coordinator.

If you believe any OMPP staff members or contractors are not in compliance with any provision contained within the *Security Rule*, either intentionally or unintentionally, please notify the OMPP Security Coordinator.

OMPP Security Coordinator: Jenifer Nelson at (317) 232-4305

Deleted: *7.02*

Deleted: *10*

Section 2: Organizational Requirements

Purpose

To define the type of entity FSSA, and OMPP, represents; and to identify associated organizational requirements that apply.

Policy

FSSA and OMPP Designation

FSSA has been designated as a hybrid entity; OMPP has been designated as a health care component of FSSA, and is therefore referred to as the covered entity. Certain organizational requirements will apply to FSSA, since electronic protected health information (PHI) is maintained, created, received, or transferred by or on behalf of the health care component of the covered entity (OMPP).

Documentation

FSSA has designated itself a hybrid entity and has designated OMPP a covered entity. OMPP is not an affiliated entity. As the covered entity, OMPP is subject to the Security Rule.

The OMPP security coordinator will maintain a copy of that designation.

Safeguard Requirements

OMPP will only disclose PHI to another component of FSSA the minimum necessary for the administration of the program, and only after the other component agrees to follow the same rules that govern OMPP and that are specified in the provisions of a Memorandum of Understanding (MOU).

The Security Coordinator in OMPP will maintain a listing of the other components that receive PHI, and verify that those components agree to protect the PHI.

Deleted: *7.02*

Deleted: *10*

Procedure

Documentation of Designation

OMPP is a covered entity, and the OMPP Security Coordinator will maintain that documentation for six years from the date of its creation or the date when it last was in effect, which ever is later.

Providing PHI to other components of FSSA

Prior to providing any PHI to other FSSA components not designated as the covered entity, the OMPP Security Coordinator must be notified to ensure that the other FSSA components to receive the PHI agree to protect the PHI under the same rules as OMPP (as verified in an MOU).

Questions

Any questions regarding the organizational requirements of OMPP or another component of FSSA should be directed to the OMPP Security Coordinator.

Regulatory Requirements and Authority: 45 CFR 164.105

Deleted: *7.02*

Deleted: *10*

Section 3: Security Management

Purpose

To issue instructions to all OMPP staff regarding the policy and procedures relating to general security management procedures in place to ensure compliance with the *Security Rule* and to prevent, detect, contain and correct security violations.

Policy

Designated Security Officials

FSSA has a Security Office; OMPP will coordinate with this existing office.

OMPP will designate a Security Coordinator, to be held by a qualified member of OMPP with appropriate experience. That designation will be made known to all OMPP Staff.

Risk Analysis

The OMPP conducted an initial assessment of security in 2001, which was later updated in 2003. OMPP also conducted a poll of the workforce to determine risks for completion of a thorough risk assessment. All identified risks were reviewed and ranked according to the probability of occurrence and impact. A determination was then made regarding the need for implementing additional steps to address each of the identified risks.

The OMPP Security Coordinator, or a designated delegate, will continue to conduct re-assessments as appropriate.

Assessments will highlight potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by OMPP. Such assessments will be used by the OMPP to modify risk management processes, as appropriate, to ensure continued compliance with the *Security Rule.*

Deleted: *7.02*

Deleted: *10*

Risk Management Processes

OMPP will implement sufficient security measures to reduce risks across the full range of security issues, as appropriate and in compliance with the *Security Rule*. Measures will include the following:

- Periodic technical and non-technical evaluations in response to environmental and/or operational changes affecting the security of electronic PHI, to ensure that all security policies and procedures continue to meet the requirement of the *Security Rule*.

- Ongoing evaluations of the security of electronic PHI, both technical and non-technical to include access management procedures which examine:
    - Physical access to electronic PHI via a computer or other media device, in addition to those facilities and/or individual workstations which house such electronic PHI, and
    - System activity reviews.

- Security awareness and training programs with certification requirements will be required for all workforce members.

- In accordance with the **FSSA HIPAA Sanction Policy # AD1-17**, sanctions may be applied against those workforce members who fail to comply with the security policies and procedures as contained in this manual.

FSSA AD1-17

The OMPP Security Coordinator will maintain the responsibility to evaluate, monitor and modify security measures as deemed appropriate.

Procedure

Security Assessments

The designated OMPP Security Coordinator, or a designated delegate, will continue to conduct re-assessments as appropriate.

Ongoing Evaluation of Security Measures

The OMPP Security Coordinator will maintain the responsibility to evaluate, monitor and modify security measures as appropriate.

Deleted: 7.02

Deleted: 10

Security updates and/or reminders will be provided to OMPP staff, by the OMPP Security Coordinator, on a periodic basis.

Information System Activities

OMPP Supervisors will maintain the responsibility to monitor information system activities of assigned workforce members and impose sanctions, as detailed in Section 15, to workforce members who are conducting improper activities.

Questions

Any questions regarding the security management processes in place to monitor electronic PHI should be directed to the OMPP Security Coordinator.

Regulatory Requirements and Authority: 45 CFR 164.308

Deleted: *7.02*

Deleted: *10*

Section 4: Workforce Security

Purpose

To issue instructions to all OMPP staff regarding the policy and procedures relating to maintaining personnel security, specifically to prevent those workforce members who do not have access to PHI from obtaining access to electronic PHI, while permitting appropriate access to those members authorized to have such access. This includes ensuring that maintenance and other personnel have proper authorization after receiving security training when working in locations where electronic PHI resides.

Policy

Responsibility of OMPP regarding Access

All OMPP staff, including interns and other support staff, who will have access to OMPP locations where PHI is housed, will be given access to such locations where electronic PHI is housed, and will receive security training and authorization by appropriate management within OMPP and/or FSSA. The OMPP Security Coordinator will coordinate with the Indiana Department of Administration (IDOA) to ensure that maintenance and janitorial staff, with access to OMPP locations where electronic PHI is housed, are properly trained. All OMPP staff members that are given access to locations where electronic PHI is housed will be trained on environmental protections required of them when working in locations where electronic PHI resides. Training documentation will be maintained by the OMPP Security Coordinator.

Access Controls for Staff not Authorized to access electronic PHI

OMPP supervisors will maintain the responsibility to monitor respective staff members, and to ensure that the access of a workforce member to electronic PHI or access to those locations where electronic PHI is housed is appropriate.

All authorizations to access electronic PHI or facilities where electronic PHI is housed, will be maintained by the OMPP Privacy Coordinator and/or OMPP Security Coordinator.

Deleted: 7.02

Deleted: 10

Termination of Access

OMPP supervisors will maintain responsibility for termination of access to locations where electronic PHI is housed. Access must be terminated when the employment of a workforce member ends, or job functions are modified to the extent that access requirements end or change. Termination of access, or change of access, must occur prior to or on the same day that employment ends or job functions change. The OMPP Security Coordinator will be notified of access termination or changes.

The OMPP Privacy Coordinator and/or Security Coordinator will be notified by the respective supervisor, and will be responsible for ensuring that access in MMIS and/or facility access will be terminated as needed. The OMPP Privacy Coordinator and/or Security Coordinator will maintain all relevant documentation regarding such termination of access.

Procedure

Access Procedures

Access to locations where electronic PHI is housed will be granted by respective supervisors. Appropriate authorization to secure areas, and security training documentation will be maintained by the OMPP Security Coordinator and/or Privacy Coordinator.

Termination Procedures

The OMPP Privacy Coordinator and/or Security Coordinator will maintain all relevant documentation regarding termination of access to facilities where electronic PHI is housed.

Access Termination

The OMPP Security Coordinator will be responsible for coordinating with all entities to terminate physical or technical access as appropriate.

Access Controls for Operational / Maintenance Personnel

The OMPP Security Coordinator will coordinate with IDOA to ensure that maintenance, janitorial, and other support staff are properly trained prior to being given access to OMPP locations where PHI resides. Training materials will be provided by the FSSA Security Manager and the OMPP Security Coordinator.

Deleted: *7.02*

Deleted: *10*

Questions

Any questions regarding processes in place to monitor workforce security should be directed to the OMPP Security Coordinator.

Regulatory Requirements and Authority:

45 CFR 164.308(a)(3)(i)-(ii)

Deleted: *7.02*

Deleted: *10*

Section 5: Security of Information Systems

Purpose

To issue instructions to all OMPP staff regarding the policy and procedures relating to the security of information systems to ensure that all workforce members have appropriate access to information systems that contain electronic PHI, and that secure electronic information systems which house electronic PHI are maintained.

Policy

Access to Electronic PHI

Access to electronic PHI will be granted to authorized OMPP staff members. Prior to receiving access, approval must be obtained by the appropriate management, and all authorizations will be maintained by the OMPP Security Coordinator (and/or Privacy Coordinator).

The respective OMPP supervisors will be responsible for ensuring that all members of his or her workforce receive appropriate access to electronic PHI, receive appropriate and timely training on security and the use of such electronic PHI, and that access rights are reviewed and modified accordingly.

Policies will be implemented, based upon OMPP's access authorization policies, to grant access to electronic PHI through access to a workstation, transaction, program or process.

Minimum Necessary Requirements

Electronic access to PHI will be limited to the minimum necessary required to perform job duties. The respective OMPP supervisors will be responsible for reviewing and controlling their staff member's access to electronic PHI.

Access Establishment and Modification

Policies have been implemented, based upon OMPP's access authorization policies, to review and modify a user's right of access to a workstation, transaction, program or process.

Deleted: *7.02*

Deleted: *10*

Termination of Electronic Access

OMPP supervisors will be responsible for ensuring that all members of his or her workforce have appropriate access to electronic PHI, and that such access is terminated when the employment of a workforce member ends, or job functions are modified to the extent that access requirements end or change.

When a workforce member terminates employment for whatever reason, the OMPP Privacy Coordinator and/or Security Coordinator will be notified by the respective supervisor prior to or on the same day of employment termination, and will be responsible for ensuring that access in MMIS will be terminated. The OMPP Privacy Coordinator and/or Security Coordinator will maintain all relevant documentation regarding such termination of access.

Electronic System Reviews

Records of information system activity, such as audit logs, access reports, and security incident tracking reports will be monitored. These reports will be reviewed, as appropriate, by the OMPP Security Coordinator, and will be forwarded to OMPP supervisors as needed.

Password Management

OMPP staff members have unique passwords to access electronic PHI, and are required to change passwords every 30 days. OMPP staff members are required to safeguard their passwords, which includes not sharing passwords and not writing passwords down.

Log-In Monitoring

Policies and procedures will be implemented to monitor failed log-in attempts. The various applications will maintain systems to cease log-in attempts after 3 times if the user name and password do not match after 3 consecutive attempts to log-in. At that time, the user will be required to verify their identity by correctly answering predetermined questions to regain access to their application.

The OMPP Security Coordinator will coordinate with various system administrators and maintain documentation of any inappropriate attempts to log-in, to be handled as necessary.

Protection from Malicious Software

OMPP staff will be prohibited from installing any unauthorized software on their computers. Any unauthorized software will be reported to respective supervisors and the OMPP Security Coordinator. The OMPP Security Coordinator, in coordination with DTS, will be responsible for enforcing that all unauthorized software is deleted.

Deleted: 7 02

Deleted: 10

Virus protection software will be installed on all computers. Due to the potential security risks involved, OMPP staff are not authorized to use or to bring in media from the outside (such as disks) for use on their equipment.

Responsibility of Workforce Members

It is the responsibility of all OMPP staff to uphold all security measures in accordance with the *Security Rule*.

Workforce members will be responsible for reporting any security incidents to the OMPP Security and/or Privacy Coordinator.

Workforce members will be monitored by the OMPP Security and/or Privacy Coordinator on an ongoing basis.

The OMPP Security Coordinator will be notified of any workforce members who fail to comply with security standards.

Unauthorized Use of Electronic PHI

Any unauthorized use of electronic PHI by an OMPP staff member will be subject to the sanctions set forth for breach of security. Refer to Section 15, Sanctions, for additional information.

Procedure

Obtaining Access to Electronic PHI

OMPP workforce members will be granted access to electronic PHI through their respective supervisors and the OMPP Security Coordinator.

The OMPP Security Coordinator will coordinate with various system administrators to secure appropriate access.

Terminating Access to Electronic PHI

OMPP supervisors will be responsible for coordinating with the OMPP Security Coordinator to terminate an OMPP staff member's access to systems, which access electronic PHI, on the same day or prior to such termination.

The OMPP Security Coordinator will maintain the responsibility for coordinating with various system administrators to remove access.

Deleted: *7.02*

Deleted: *10*

Indiana*AIM* Access Monitoring

On a periodic basis, all IHCP management staff will review the Indiana*AIM* class summary for their business unit, in relation to PHI access via Indiana*AIM*, in order to answer the following questions:

- Are the Indiana*AIM* profiles for the workforce classes in their respective units, specifically those that provide access to member PHI, still necessary for staff to perform their work functions?
- Are the actual Indiana*AIM* access classes currently assigned to the staff members in their units the same in comparison to the pre-assigned profiles for the workforce class for each staff member?
- Are all staff members assigned to the unit classes currently working in the unit?
- Are any staff members who currently work in the unit, but are not listed on the quarterly profile for the business unit, assigned to another unit's access class?

Modification to Indiana*AIM* classes

For any change needed to modify the Indiana*AIM* access profiles for the work unit, the IHCP manager will notify the AIM Security Manager of the needed change. Confirmation of appropriate access or modification is required to be submitted to the AIM Security Manager.

For any staff member found to be on the unit access profile who is not currently working in the unit, notify the AIM Security Manager of the need to delete all Indiana*AIM* access for that staff member.

Password Requirements

OMPP, in coordination with various systems, will require, through a built in systems requirement, that staff members change passwords every 30 days.

Log-In Monitoring

OMPP, in coordination with various systems, will maintain built in system controls to cease log-in attempts after 3 times if the user name and password do not match after 3 consecutive attempts to log-in..At that time, the user will be required to verify their identity by correctly answering predetermined questions to regain access to their application.

The OMPP Security Coordinator, in coordination with various system administrators, will maintain all documentation of any inappropriate attempts to log-in, and will follow up as deemed necessary.

Deleted: *7.02*

Deleted: *10*

Questions Any questions regarding processes in place to monitor the security of information systems should be directed to the OMPP Security Coordinator.

Regulatory Requirements and Authority:
45 CFR 164.308(4) and 164.308(5)

Deleted: 7.02

Deleted: 10

Section 6: Security Training and Awareness

Purpose

To provide instructions regarding training requirements, specific to security, required of all OMPP staff in regard to HIPAA security regulations.

Policy

All OMPP staff members, including all management staff, will participate in a security awareness and training program, and will be certified in the HIPAA *Security Rule*.

Procedure

Training Requirements

Each OMPP section supervisor is required to notify the OMPP Security Coordinator of the actual start date of any new workforce member included in the respective section.

The OMPP Security Coordinator will be responsible for ensuring that all staff, including existing staff and new staff that will join OMPP in the future, participates in a security awareness and training program, and receive a passing score on the post-training evaluation. Training components will address, in detail, all components contained in this manual.

New staff members will be required to receive training within the first two weeks of employment.

Re-Training

The OMPP Security Coordinator will be responsible for ensuring that all staff are re-trained and re-certified periodically.

Deleted: *7.02*

Deleted: *10*

Documentation

The OMPP Security Coordinator will maintain all records to document training, certification, and re-training.

Role of the OMPP Supervisors

The respective OMPP supervisors will be responsible for ensuring that all members of his or her workforce are sufficiently trained in security, and in the appropriate use and handling of PHI.

Security Updates

The OMPP Security Coordinator will be responsible for providing periodic security updates to all OMPP staff members, as determined appropriate.

Questions

Any questions regarding processes in place to monitor the security of information systems should be directed to the OMPP Security Coordinator.

Regulatory Requirements and Authority: 45 CFR 164.308(5)(i)

Deleted: *7.02*

Deleted: *10*

Section 7: Security Incidents

Purpose

To issue instructions to all OMPP staff regarding the policies and procedures required of them to ensure security incidents are documented and responded to in accordance with the *Security Rule*, and in compliance with Indiana Code 4-1-11.

Deleted:

Policy

Responsibilities of the OMPP

The OMPP workforce will be responsible for identifying, documenting, and responding to all suspected or known security incidents. The OMPP will also be responsible for the disclosure of any breach of the security of the system to the affected parties, in accordance with IC 4-1-11.

Formatted: Font: 12 pt

Formatted: Font: 12 pt

Formatted: Hyperlink, Font: 12 pt

The OMPP Security Coordinator will be responsible for including these policies and procedures to document such incidents in the training materials that will be distributed to all OMPP workforce members.

Responsibilities of Staff

Each OMPP workforce member will be responsible for reporting any known security incidents, and for documenting the outcome of each security incident. The *OMPP Privacy/Security Incident Form* should be used for each known incident (see Appendix B).

Documentation of Incidents

All security incidents are to be documented using the *OMPP Privacy/Security Incident Form* (see Appendix B). Staff may transmit this form to the OMPP Security Coordinator using the form provided on the shared drive. Documentation will be maintained by the OMPP Security Coordinator.

Examples of Incidents

Examples of security incidents include (not limited to):

- Improper network activity
- Misuse of electronic data
- Unauthorized access to OMPP work areas

Deleted: 7.02

Deleted: 10

- Unsupervised access to OMPP work areas
- Security breach of computerized data

Formatted: Bullets and Numbering

Deleted: <#>¶

Procedure

Reporting of Security Incidents

All workforce members will report any known or suspected security incidents to the OMPP Security Coordinator, using the *OMPP Privacy/Security Incident Form* (see Appendix B). All suspected incidents must be reported; if a workforce member is not certain that an event constitutes an incident, it should be reported.

Staff may transmit the *OMPP Privacy/Security Incident Form* to the OMPP Security Coordinator using the form provided on the shared drive.

The OMPP Security Coordinator will notify the FSSA Security Office of each incident, and will maintain all documentation.

Mitigation of effects

The OMPP must mitigate, to the extent practicable, any harmful effects of the security incidents that are known to the covered entity.

Disclosure of Security Breach

The OMPP must disclose a breach of the security of the system on a timely basis, in writing or by electronic mail, following discovery or notification of the breach, to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

If the cost of providing such notice is at least two hundred fifty thousand dollars ($250,000) and the number of persons to be notified is at least five hundred thousand (500,000); or if OMPP does not have sufficient contact information, then OMPP may use an alternate form of notice as follows:
(1) Conspicuous posting of the notice on the state agency's web site if the state agency maintains a web site; or
(2) Notification to major statewide media.

Formatted

Formatted: Font: 12 pt

Formatted: Hyperlink, Font: 12 pt

Formatted: Font: 12 pt

Field Code Changed

Formatted: Font: 12 pt

Formatted: Space Before: 0 pt, After: 0 pt

Formatted: Font: 12 pt

If OMPP provides notice to more than one thousand (1,000) individuals, OMPP shall notify without unreasonable delay all consumer reporting agencies (as defined in 15 U.S.C. 1681a) of the distribution and content of the notice.

Deleted: 7.02

Deleted: 10

The OMPP Security Coordinator will coordinate and ensure that all required disclosures are made to affected state residents and consumer reporting agencies, as appropriate, and will maintain documentation of those disclosures with the OMPP Privacy/Security Incident Form (Appendix B).

Formatted: Font: 12 pt

Formatted: Font: 12 pt

Questions Any questions regarding processes in place to report security incidents should be directed to the OMPP Security Coordinator.

Regulatory Requirements and Authority: 164.308(6)(i)-(ii) and Indiana Code 4-1-11

Deleted: 7.02

Deleted: 10

Section 8: Contingency Plan

Purpose

To issue instructions to all OMPP workforce members regarding the policies and procedures in place for responding to an emergency or other occurrence that damages systems that contain electronic protected health information.

Policy

Applications and Data Criticality Analysis

OMPP's primary objective is to maintain the ability of providers to provide services to Medicaid patients (identify Medicaid eligibles and pay claims). In general, OMPP's business functions are contracted out to a fiscal agent and other contractors. In these circumstances, OMPP will ensure that contracted functions are included in the contractors' contingency plan as appropriate, and that OMPP's contingency plan addresses OMPP activities needed to support contracted functions.

OMPP units that are responsible for critical processes will be identified and given priority to access facilities and electronic systems during emergency operation mode. Specific subsystems within MMIS will be given priority in restoring normal operations for critical functions.

All OMPP data systems will be identified and classified based on the criticality in relationship to the primary objective of OMPP, and will be included in the contingency plan accordingly.

The *Office of Medicaid Policy and Planning Business Continuity and Contingency Plan* (BCCP) document will detail OMPP's official contingency plan, which will be driven by the data criticality analysis. A link to this document is provided on page 8-3.

Data Backup Plan

In general, PHI should be stored on the users' home drive. PHI that is stored on the servers that are maintained within the FSSA network is backed up. It is the responsibility of the user to back up their hard drive on a regular basis.

Based on the data criticality analysis, OMPP, in coordination with various system administrators, will implement procedures to create and maintain retrievable exact copies of electronic PHI.

Deleted: *7.02*

Deleted: *10*

The fiscal agent and other contracted entities have data backup plans for their respective systems, which will not be addressed within this manual.

Off-Site Disaster Recovery Plan

OMPP will establish procedures to restore any loss of data as needed and as appropriate based on the data criticality analysis.

Emergency Mode Operation Plan

OMPP will ensure continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

Key OMPP staff will be instructed on what data is available and where to access data from (fiscal agent site, etc.) during emergency operation mode.

The OMPP Security Coordinator, or a delegated staff member, will be responsible for coordinating access to and maintaining the security of PHI during emergency operation mode.

Testing and Revision Procedures

The OMPP Security Coordinator or a delegated staff member will, on at least an annual basis, conduct and document the following processes:

- Review and revision of written OMPP contingency plans, and
- Testing of at least some component of the contingency plan.

Procedure

Ownership

Determine all data collected, obtained, and stored by OMPP and the associated owner for each data component. Determine data collected, obtained, and stored by contracted vendors and identify ownership of such data, and OMPP functions critical to the continuation of contracted functions.

Classify data as being the master file, permanent record, or extract file.

Deleted: 7.02

Deleted: 10

Protected Nature

Determine the level of confidentiality and classify data components based on level: Protected (PHI), Sensitive, and Public Information.

Criticality

Determine and classify business functions and associated data components necessary to perform those business functions. Classify based on which business functions are required to occur on an immediate, daily, weekly, or longer basis. Implement back up procedures consistent with criticality classification.

Location of Data

Determine where each data component determined to be the master file and/or permanent record is stored and backed up to, and identify those critical elements that require off-site storage.

Assign Responsibility

Identify who will hold responsibility for backing up data determined to be the master file and/or permanent record, and who will access information during a contingency mode of operation.

Responsibility of OMPP Units

The *Office of Medicaid Policy and Planning Business Continuity and Contingency Plan (BCCP)* should be referenced for specific instruction, roles, and responsibilities of individual units within OMPP. The current version of the BCCP is attached below:

BCCP Jan07

Questions

Any questions regarding OMPP's contingency plan should be directed to the OMPP Security Coordinator.

Regulatory Requirements and Authority: 45 CFR 164.308(7)(i)-(ii) and 45 CFR 164.310(a)(2)(i)

Deleted: *7.02*

Deleted: *10*

Section 9: Business Associate Contracts and Other Arrangements

Purpose

To issue instructions to all OMPP workforce members regarding the policies and procedures in place for ensuring that all business associates are in compliance with the *Security Rule*.

Policy

Business Associates (defined)

A person or organization that performs a function or activity on behalf of the IHCP, but is not part of the FSSA/OMPP staff, such as the fiscal agent or other contracted entities.

Note: A Memorandum of Understanding (MOU) is required, as opposed to a Business Associate Agreement, if electronic PHI is provided to another government entity, including another component of FSSA outside of OMPP. FSSA Policy # AD1-18 requires all FSSA divisions to adhere to relevant HIPAA policies regarding the use or disclosure of PHI.

PDF Adobe
FSSA AD1-18

Business Associate Agreement

The language in the business associate agreement requires the business associate to adhere to all federal and state laws and statutes for the security of electronic PHI. Any HIPAA Security language developed by OMPP shall be approved by the FSSA HIPAA Privacy Official. The OMPP Security Coordinator will review this language to ensure that security of electronic PHI is appropriately addressed. All relevant contracts will contain this language specific to security of electronic PHI.

The contract between OMPP and a business associate must specify that the business associate will:

- Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health

Deleted: 7.02

Deleted: 10

information that it creates, receives, maintains, or transmits on behalf of OMPP as required by the *Security Rule*;

- Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
- Report to OMPP any security incident of which it becomes aware; and
- Authorize termination of the contract OMPP, if OMPP determines that the business associate has violated a material term of the contract.
- Implement a disaster recovery plan, as appropriate, which includes mechanisms to recover data and/or alternative data storage sites, as determined by OMPP to be necessary to uphold integral business functions in the event of an unforeseen disaster.

Memorandum of Understanding

If the Business Associate is another government entity, the OMPP is in compliance if it enters into a memorandum of understanding (MOU) with the business associate, if this MOU contains terms to ensure that security of PHI is appropriately addressed and that the entity receives only the minimum necessary PHI.

Safeguard requirements related to group health plans do not apply to OMPP, as OMPP is not a group health plan.

Breach or Violation by a Business Associate

If OMPP learns that a business associate has materially breached or violated the satisfactory assurance of its business associate contract, OMPP must take prompt, reasonable steps to see that the breach or violation is cured. If the business associate does not promptly and effectively cure the breach or violation, OMPP must coordinate with FSSA's legal department to terminate the contract with the business associate, or if contract termination is not feasible, report the business associate's breach or violation to Health and Human Services.

BAA/MOU Determinations

Any review process to determine the nature of a HIPAA business associate relationship (or MOU) shall be coordinated by the OMPP Security Coordinator and the FSSA HIPAA Security Manager (or the FSSA HIPAA Privacy Official).

Exclusions, to which this standard will typically not apply, include the following:

Deleted: *7.02*

Deleted: *10*

- With respect to disclosures by the IHCP to a health care provider concerning the treatment of a member; or

- With respect to uses or disclosures by the IHCP, county caseworkers, and staff who maintain the Indiana Client Eligibility System (ICES) as they relate to the determination of member eligibility and enrollment in the IHCP.
- Neither providers nor the local office of Family and Children are considered "business associates" under HIPAA.

Procedure

Releasing Electronic PHI to Business Associates

Business associates may require electronic PHI to effectively perform contracted functions of OMPP. Electronic PHI may be disclosed to business associates only to perform authorized functions **as specified in the approved business associate provisions in the contract.**

Releasing PHI to another Government Entity

When the business associate is another government entity, or another component of FSSA outside of OMPP, a Memorandum of Understanding (MOU) is required between OMPP and the other entity or other component of FSSA. Electronic PHI may be disclosed to such entities only to perform authorized functions as specified in the MOU.

Business Associate Violations

OMPP staff should report any known material breach or violation of a business associate to the OMPP Security Coordinator using the *OMPP Privacy/Security Incident Form* (Appendix B). The official form is located on the shared drive.

Mitigation

OMPP must mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of electronic protected health information in violation of policies and procedures, or of any requirements contained with the *Security Rule*, by a business associate.

Questions

Any questions regarding release of electronic PHI to business associates or other government entities should be addressed to the OMPP Security Coordinator.

Regulatory Requirements and Authority: 45 CFR 164.308(8)(b)(1) and 164.314(a)(1)

Deleted: 7.02

Deleted: 10

Section 10: Facility Access Controls

Purpose

To issue instructions to all OMPP staff regarding policies and procedures associated with access to OMPP's electronic information systems and the facility or facilities in which they are housed.

Policy

Contingency Operations

The OMPP will implement, as needed, the disaster recovery plan and emergency mode operations plan. These plans outline procedures that allow facility access in support of restoration of lost data, in the event of an emergency. Section 8 of this manual, in addition to the *Office of Medicaid Policy and Planning Business Continuity and Contingency Plan* document, provides additional information on emergency operation protocols.

Access Control and Validation

OMPP is housed in a secure self-contained area. OMPP workforce members are authorized to enter this area through one of three doors, which require a four-digit access code for entrance. Each individual OMPP staff member has a unique access code that permits entrance into the facility.

Visitor Access

Visitor controls are in place to limit outside entrance into facilities. Visitors may enter the OMPP facility through one door, which is monitored during all operating hours by a receptionist. Visitors must be approved for entrance, sign a log of visitation, wear a visitation badge and be escorted by an authorized OMPP staff member at all times.

All OMPP staff will be responsible for assisting in controlling and validating a person's access to facilities (i.e., question unfamiliar individuals and report their presence to the Security Coordinator as needed).

Facility Access Security Plan

Only properly authorized access to OMPP's electronic information systems and the facility or facilities in which they are housed is permitted.

OMPP staff will be responsible for ensuring that all non-OMPP staff on the premises are properly authorized, as specified in this section.

Deleted: *7.02*

Deleted: *10*

During normal business hours, OMPP will be responsible for safeguarding the facility and equipment from any unauthorized physical access, tampering, and theft, through employing physical security measures as specified in the security requirements and throughout this manual. FSSA, in coordination with IDOA/Capital Police, will continue to maintain security measures for the building where OMPP resides.

Maintenance of Facilities

Any repairs or modifications to the facility (i.e., hardware, walls, doors, locks) in which OMPP is housed must be documented using the *Facility Modification Form* (refer to Appendix C). The OMPP Security Coordinator will be responsible for coordinating with IDOA for facility repairs/modifications.

Software / Hardware Maintenance

The OMPP Security Coordinator will be responsible for coordinating and authorizing any access by outside vendors (other than DTS) to software and/or hardware for the purposes of testing or revision.

Procedure

Contingency Operations

In the event of an emergency, the OMPP Security Coordinator will monitor access to OMPP to ensure only appropriate non-OMPP staff are granted access.

Access Controls

Physical access will be limited to only authorized staff. Currently, physical access is controlled through the use of key pad devices, with unique entrance codes assigned to individual OMPP workforce members. Access control devices may be modified in the future to incorporate updated devices, as appropriate.

Visitor access will be limited to one entrance area. Visitations will be documented, and all visitors must wear visitation badges and be escorted by an authorized OMPP staff member while on OMPP premises.

Access by individuals for the purpose of software and/or hardware testing and revision must be coordinated through the OMPP Security Coordinator.

Deleted: *7.02*

Deleted: *10*

Access by authorized contracted vendors will be provided within a defined location, which has appropriate computer workstations.

Facility Modifications The OMPP Security Coordinator will approve all repairs and modifications of the OMPP facility related to security, and will maintain records, which document any changes made after the date of this manual, using the *Facility Modification Form* (refer to Appendix C).

Questions Any questions regarding facility access controls should be addressed to the OMPP Security Coordinator.

Regulatory Requirements and Authority: 45 CFR 164.310(a)

Deleted: *7.02*

Deleted: *10*

Section 11: Workstation Use and Security

Purpose

To issue instructions to all OMPP staff regarding the policy and procedures relating to the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic protected health information.

Policy

Approved use of workstations

OMPP staff members are permitted to use workstations to perform only authorized duties specific to their individual job functions. Respective supervisors are responsible for ensuring that OMPP staff members are properly trained on appropriate and secure uses of their workstations.

Access to workstations is limited to OMPP staff. Unauthorized visitors are not permitted to access any workstations. OMPP staff will be responsible for reporting any unauthorized users to their respective supervisor and the OMPP Security Coordinator.

Workstation Environment

OMPP staff members will be responsible for maintaining a secure personal working environment that ensures the protection of PHI from any unauthorized viewing and/or access. A "clean desk" policy will be encouraged for all OMPP staff members to ensure that PHI is adequately protected from viewing and/or access.

Physical Safeguards

Technical controls will help guard against unauthorized viewing of electronic PHI at workstations through automatic session terminations.

OMPP staff members must employ additional measures, as appropriate, to maintain a secure environment while working on electronic PHI.

Deleted: *7.02*

Deleted: *10*

Procedure

OMPP Staff Responsibilities

OMPP staff will be responsible for maintaining a secure workstation environment to maximize the security of electronic health information. This includes maintaining a "clean desk" (as appropriate), logging off of systems containing electronic PHI before leaving the workstation unattended, and positioning computer screens (if feasible) to ensure that electronic PHI is protected from unauthorized viewing.

OMPP staff will be responsible for reporting any security violations or unauthorized users to the OMPP Security Coordinator.

Responsibilities of Management

Respective supervisors and the OMPP Security Coordinator will ensure that OMPP staff have appropriate access to carryout job functions.

The OMPP Security Coordinator will periodically observe workstation attributes and recommend reasonable corrections to management, as necessary. Documentation of all workstation audits and corrections performed will be maintained by the OMPP Security Coordinator.

Questions

Any questions regarding facility access controls should be addressed to the OMPP Security Coordinator.

Regulatory Requirements and Authority: 45 CFR 164.310(b) – (c)

Deleted: 7.02

Deleted: 10

Section 12: Device and Media Controls

Purpose

To issue instructions to all OMPP staff regarding the policies and procedures surrounding maintenance of electronic media that contain electronic protected health information, specifically that related to receipt, removal, and movement of such media.

Policy

Moving of Hardware or other Media Containing Electronic PHI

OMPP staff members are not permitted to use any unauthorized hardware. The OMPP Security Coordinator maintains the responsibility for governing receipt and approval of all hardware that contains PHI (computer system hardware).

OMPP staff members are not authorized to re-locate authorized hardware without prior approval from the OMPP Security Coordinator. This includes relocating hardware out of a facility, in addition to movement of hardware within the facility. The *Notification of Transferred Equipment and/or Furniture SF44129* form (see Appendix D) must be completed and authorized by the OMPP Security Coordinator prior to relocating hardware within the facility, out of the facility, or prior to discarding of any hardware or other media containing electronic PHI.

The OMPP Security Coordinator will maintain a record of all movements of hardware and electronic media, and any person responsible thereof.

Formatting of Disks

Only authorized staff will format computer hard drives. The OMPP Security Coordinator will maintain the responsibility of coordinating this task.

OMPP staff will be permitted to format and reformat computer media devices, which includes CDs, diskettes, floppy disks, and USB storage devices, as needed for the purposes of performing their position's responsibilities.

Deleted: *7.02*

Deleted: *10*

Removal of Equipment

DTS will be responsible for removing electronic PHI stored on computer media, which includes CDs, diskettes, floppy disks, and USB storage devices, as needed. Prior to disposal, the OMPP staff member is responsible for saving any needed PHI on the home drive.

Hardware drives located within OMPP that need to be destroyed must be coordinated with DTS through the OMPP Security Coordinator, and must be documented using the *Notification of Transferred Equipment and/or Furniture SF44129* form. The Security Coordinator is responsible for coordinating destruction of hardware with the Division of Technology Services (DTS).

Data Backup and Storage

All OMPP staff will save work to their home drives, which will be backed up on a regular basis.

Procedure

Hardware Changes

OMPP office automation staff will notify the OMPP Security Coordinator, and will complete the *Notification of Transferred Equipment and/or Furniture SF44129* form for the purpose of approving and coordinating the following activities:

- Receipt of new hardware
- Formatting of hard drive
- Movement of existing hardware
- Disposal of existing hardware

Accountability

The OMPP Security Coordinator will maintain responsibility for coordination of the above activities, as appropriate, and will maintain a record of all movements of hardware and other electronic media, and the person responsible thereof.

Changes to Tapes/Disks

OMPP workforce members, in coordination with DTS, will maintain responsibility for removing electronic PHI from media devices such as CDs, tapes and/or disks. Formatting of CDs, tapes and/or disks will be performed by OMPP workforce members.

Deleted: 7.02

Deleted: 10

OMPP staff members maintain responsibility for ensuring that all media containing electronic PHI is placed in the designated container, and DTS will be responsible for ensuring that PHI is removed prior to disposal of computer media, or prior to using such devices for other purposes.

Prior to disposal, the OMPP staff member is responsible for saving any needed PHI to the home drive.

Data Backup and Storage

All workforce members will save work to their home drive, which will be backed up on a regular basis. Any work saved elsewhere must be backed up by the user as necessary.

Questions

Any questions regarding device and media controls should be addressed to the OMPP Security Coordinator.

Regulatory Requirements and Authority: 45 CFR 164.310(d)

Deleted: *7.02*

Deleted: *10*

Section 13: Technical Controls

Purpose

To issue instructions to all OMPP staff regarding the policy and procedures for access of electronic information systems that maintain electronic protected health information, to allow access only to those persons or software programs that have been granted access rights.

Policy

User Authentication

OMPP staff members will be assigned unique user names and/or numbers which will be used for authentication of the user and for identifying and tracking user identity and associated activities, as appropriate. Access to AIM will be granted through OMPP; access to the FSSA network will be secured through DTS.

Any changes made to the user name assignment mechanisms used by DTS or FSSA will be incorporated by OMPP.

Technical Emergency Access

OMPP staff members should contact the DTS helpdesk to resolve technical access issues that are not OMPP-wide (i.e., individual access issues). DTS should be contacted to resolve technical access issues that are OMPP-wide.

If an OMPP network is down or is destroyed, the OMPP Security Coordinator should be contacted. Necessary electronic PHI can be obtained for continuation of business processes in an emergency through the OMPP Security Coordinator, who will be responsible for coordinating with DTS, the fiscal agent, and other contractor(s) to obtain emergency access to needed information.

Access to electronic data housed at the fiscal agent site, or other locations, will be available to appropriate OMPP staff in the event of contingency mode operations. These locations operate as secure facilities. OMPP staff will be admitted to these locations to perform critical functions, as outlined in the *Office of Medicaid Policy and Planning Business Continuity and Contingency Plan (BCCP).*

Deleted: *7.02*

Deleted: *10*

Automatic Log-off Controls

Computer screens at individual OMPP staff workstations will time out (inactivate) after fifteen minutes of inactivity on the FSSA LAN to safeguard against unauthorized viewing, requiring a password to be entered to regain access. Automatic log-off controls for the FSSA LAN are consistent with FSSA policy.

Indiana*AIM* access will inactivate after eight minutes of inactivity.

Other electronic sessions to systems housing electronic PHI will be terminated after a 15 minute period of inactivity, requiring the user to log on to systems again when access is once again needed. These automatic log-off controls are consistent with the FSSA-wide policy.

Type of Connection	Period of inactivity for session termination
FSSA LAN	15 Minutes
Indiana*AIM*	8 Minutes
Other applications/connections to access PHI	15 Minutes

Encryption and Decryption

Data is stored within the secure State network. Any transmissions made within FSSA are secure.

OIT established the standard for encryption. OMPP will use the OIT standards for encryption.

Integrity Controls for Electronic PHI

Various mechanisms will be used by OMPP management and contracted vendors to monitor the integrity of electronic PHI.

Practical controls will be utilized to ensure that all access to electronic PHI is granted through an approved process. This process will require that authorization to alter/modify electronic PHI is limited to specific staff members within OMPP, as appropriate and necessary to perform job functions.

Database controls will be utilized to ensure that no inappropriate modifications are made to electronic PHI. These controls are built into the system.

Deleted: 7.02

Deleted: 10

DTS will be held responsible for integrating technical integrity controls to ensure for a secure network.

The OMPP Security Coordinator will receive reports on system activity, and changes made to information, to routinely record and examine activity of information systems containing or using electronic PHI.

Additional integrity controls will be used by contracted vendors, such as the fiscal agent, to monitor system traffic and changes made to data elements.

OMPP business associates will be contractually obligated to not improperly modify PHI for which they are granted access.

Authentication of Electronic Access

Electronic access to systems containing PHI will be limited to onsite access by OMPP staff members with assigned unique user names and/or numbers.

Off-site, or remote access for individual staff members of OMPP, is not allowed unless specifically approved by the OMPP Security Coordinator. Remote access will be granted to OMPP staff only as necessary. Remote access could be made available to approved staff members through a secure virtual private network (VPN).

Off-site or remote access for corporate entities will also utilize a secure method for transmitting/receiving data. The OMPP Security Coordinator will hold responsibility for coordinating all corporate remote access.

Transmission Security

PHI communicated via e-mail text or attachments, to any FSSA/OMPP staff member or external entity, should always be limited to the minimum necessary amount of information that is needed exclusively to carry out treatment, payment, or operations (TPO). E-mail transmissions of PHI must only be made to individuals who are authorized to receive such information, and files containing PHI that are exchanged with outside entities (i.e., outside of the secure State network) should be encrypted with the "Certified Mail" tool, or the currently approved OMPP encryption tool. In addition, the following statement will be systematically generated at the bottom of all email messages:

"The information contained in this E-mail and/or attachments may contain protected health, legally privileged, or otherwise confidential information intended only for the use of the individual(s) named above. If you, the reader of this message, are not the intended recipient, you are hereby notified that you may not further disseminate, distribute,

Deleted: 7.02

Deleted: 10

disclose, copy or forward this message or any of the content herein. If you have received this E-mail in error, please notify the sender immediately and delete the original."

All questions concerning e-mail transmission of PHI are to be referred to the OMPP Security Coordinator for resolution.

Procedure

Responsibilities of Management

Respective supervisors and the OMPP Security Coordinator will ensure that OMPP staff members are assigned unique user names/numbers and have access only to that information which is needed to perform job functions.

Access to Electronic Systems

OMPP will establish additional security controls for key personnel, as deemed appropriate, to restore network access in the event that all known local accounts are deliberately disabled.

Review of System Activity

The OMPP Security Coordinator will be responsible for reviewing and/or coordinating with OMPP supervisors for the review of system activity reports.

Remote Access

The OMPP Security Coordinator will be responsible for reviewing all corporate and individual off-site/remote access requests, and for providing authorization if a determination is made that such access is needed. This access may be made available through a secure VPN.

Emergency Facility Access

The OMPP Security Coordinator holds responsibility for coordinating emergency access to outside facilities, as needed to continue business functions that are outlined in the *Business Continuity and Contingency Plan* (attached).

BCCP Jan07

Questions

Any questions regarding facility access controls should be addressed to the OMPP Security Coordinator.

Regulatory Requirements and Authority: 45 CFR 164.312

Deleted: 7.02

Deleted: 10

Section 14: Documentation Requirements

Purpose

This section of the manual details policies and procedures related to maintenance of documentation of certifications, activities, and/or assessments as required by the *Security Rule*.

Policy

Availability of the Security Policies and Procedures Manual

The OMPP Security Coordinator maintains the *HIPAA Security Policy and Procedure Manual*, and is responsible for ensuring that all OMPP staff, in conjunction with appropriate OMPP managers, are aware of the contents of this manual and have a copy of this manual available for their reference.

Training Requirements

All OMPP staff will be trained and certified on the security policies and procedures as contained in this manual. The OMPP Security Coordinator will maintain records of such training.

Updates to Manual

The OMPP Security Coordinator maintains responsibility of reviewing and/or coordinating the review of this document periodically, and updating as needed, in response to environmental or operational changes affecting the security of the electronic PHI.

Documentation

Documentation will be maintained by the OMPP Security Coordinator for six years from the date of its creation or the date when it last was in effect, whichever is later.

Documentation will be made readily available to those individuals implementing the procedures for which the documentation pertains, in addition to all other OMPP staff members.

Deleted: *7.02*

Deleted: *10*

Procedure

Distribution of Security Manual

The *HIPAA Security Policy and Procedure Manual* will be made available to all OMPP staff members through the shared network drive.

The OMPP Security Coordinator will notify staff upon any updates made to the manual.

Training

All OMPP staff members will receive computer-based training, which details all components contained within the manual. Post-training certification will ensure staff familiarity with contents of the *HIPAA Security Policy and Procedure Manual.*

Questions

Any questions regarding the *HIPAA Security Policy and Procedure Manual*, or revisions to this manual, should be addressed to the OMPP Security Coordinator.

Regulatory Requirements and Authority: 45 CFR 164.316

Deleted: *7.02*

Deleted: *10*

Section 15: Sanctions

Purpose

To issue instructions to all OMPP staff regarding the policy and procedures relating to sanctions against workforce members who fail to comply with the established security policies and procedures.

Policy

Sanctions against OMPP workforce members

OMPP is required to apply, when appropriate, sanctions against members of its workforce who fail to comply with security policies or procedures or with the requirements of the *Security Rule*.

Types of Sanctions

In accordance with the FSSA HIPAA Sanction Policy # AD1-17, OMPP workforce members may be subject to appropriate discipline for failure to comply with the relevant requirements of this policy and procedure manual.

Documentation Requirements

OMPP is required to have written policies and procedures for the application of appropriate sanctions for violations of the *Security Rule* and to document those sanctions. Sanctions related to violations of the *Security Rule* are included in FSSA personnel rules.

Documentation must be retained for a six-year period by the OMPP Security Coordinator.

Procedure

OMPP staff violation of the *Security Rule*

OMPP staff that violate the security requirement of HIPAA are subject to appropriate sanctions, which may include suspension or termination.

Deleted: *7.02*

Deleted: *10*

Role of OMPP Supervisors

Enforcement of the appropriate sanctions for OMPP staff are the responsibility OMPP management and FSSA Human Resources. The OMPP Security Coordinator and/or the FSSA HIPAA Security Manager may provide an estimate of the severity of the infraction utilizing the HIPAA regulations as a guideline, in coordination with management and/or FSSA Human Resources, as appropriate.

The OMPP supervisor is responsible for notifying the OMPP Security Coordinator of each employee security incident and sanction, for all respective employees.

Documentation Requirement

The OMPP Security Coordinator maintains the responsibility for maintaining a record of each security incident and respective sanction, as reported by OMPP supervisors.

Questions

Any questions regarding sanctions that may be imposed due to a security violation should be addressed to the OMPP Security Coordinator.

Regulatory Requirements and Authority:
45 CFR 164.308(a)(ii)(C)

Deleted: *7.02*

Deleted: *10*

Breach of the security of the system

Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a state or local agency.

The term does not include the following:

(1) Good faith acquisition of personal information by an agency or employee of the agency for purposes of the agency, if the personal information is not used or subject to further unauthorized disclosure.

(2) Unauthorized acquisition of a portable electronic device on which personal information is stored if access to the device is protected by a password that has not been disclosed.

Formatted: Font: Arial Narrow

Formatted: Font: Arial Narrow, Bold

Formatted: Heading 5

Formatted: Font: Arial Narrow, Bold

Formatted: Font: Arial Narrow

Business Associate

A person or organization that performs a function or activity on behalf of the IHCP but is not a part of the FSSA/OMPP staff, such as fiscal agent staff members, or a managed care organization's (MCO) staff members.

Covered Entity

A *covered entity* is a health plan, health care clearinghouse, or any health care provider who transmits any health information in an electronic form in connection with any HIPAA-required transactions. This includes the use of the OMNI device or direct data entry (Web entry) by a provider. Medicaid is specifically mandated as a health plan in the Act.

OMPP has been designated as a covered entity for the purposes of the Health Insurance Portability and Accountability Act (HIPAA) Standards for Security final rule.

Electronic Protected Health Information (PHI)

Protected health information (PHI) is the individually identifiable health information that is maintained in any electronic media or is transmitted by electronic media, which includes Internet, Extranet, leased lines, dial-up lines, private networks, magnetic tape, disk, or compact disk (45 CFR 162.103).

Encryption

Encryption is the conversion of data into a form, called a ciphertext that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

Deleted: *7.02*

Deleted: *10*

Indiana Health Coverage Programs (IHCP)

Includes the Family and Social Services Administration (FSSA), Office of Medicaid Policy and Planning (OMPP).

Memorandum of Understanding (MOU)

An agreement between OMPP and another component of FSSA that is required prior to disclosing PHI to another component of FSSA. PHI may only be disclosed after the other component agrees to follow the same rules that govern OMPP and that are specified in the provisions of a Memorandum of Understanding (MOU). The minimum necessary requirement also applies.

Minimum Necessary

The IHCP shall limit access and use of PHI by its staff and contractors to the minimum necessary to accomplish the defined work functions. The requirements also apply to PHI requests made by, or on behalf of, the IHCP to another covered entity.

There are instances in which the minimum necessary limitation is **not required**, including:

- Disclosures made to a member's health care provider for the purpose of providing treatment;
- Disclosures made to the member or through the member's written authorization in regard to their own PHI; or
- Uses or disclosures required by law, and when required by the Secretary of HHS to investigate or determine IHCP compliance with the *Privacy Rule*.

Protected Health Information (PHI)

Protected health information (PHI) is the individually identifiable health information that is:

- Transmitted by electronic media, which includes Internet, Extranet, leased lines, dial-up lines, private networks, magnetic tape, disk, or compact disk (45 CFR 162.103);
- Maintained in any electronic media; or,
- Transmitted or maintained in any other form or medium, which include oral communication or paper.

The IHCP is responsible for protecting the IHCP member's PHI in regard to access for use or disclosure. The majority of member information maintained on the IndianaAIM Recipient and Claim subsystems would qualify as PHI, and access must be limited to only those IHCP and contractor staff who require PHI usage in order to carry out their daily work duties. Full-time access or part-time access of limited duration, as in the case for special project work, may only be granted by the employee's supervisor and will be monitored by the supervisor on a quarterly basis.

Deleted: 7.02

Deleted: 10

Individually Identifiable Health Information

Individually Identifiable Health Information is a subset of health information, including demographic information collected from the member, and:

- Is created or received by a health care provider health plan, employer, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an member; the provision of health care to a member; or the past, present, or future payment for the provision of health care to a member; and
- That identifies the member; or
- Could reasonably be used to identify the member.

Health information includes information, whether oral or recorded in any form or medium.

PHI Exclusions

PHI excludes the individually identifiable health information in:

- Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g;
- Records used exclusively for health care treatment, for students 18 years or older or that are held by a post-secondary educational institution, and that have not been disclosed other than to a health care provider at the student's request; and
- Employment records held by a covered entity in its role as an employer.

Deleted: *7.02*

Deleted: *10*

Appendix A: Crosswalk to Security Rule Implementation Specifications

The following table illustrates where specific implementation specifications, as detailed in the *Health Insurance Portability and Accountability Act (HIPAA) Security Rule Initial Assessment*, are addressed within this manual.

Security Rule Implementation Specifications	**Where is this Implementation Specification Addressed in the *HIPAA Security Policy and Procedure Manual*?**

II. Organizational Requirements (45 CFR 164.105)

A. Health Care Component	
(1) Application of Other Provisions	Section 2: Organizational Requirements
(2) Safeguard Requirements	Section 2: Organizational Requirements
(3) Responsibilities of the Covered Entity	Section 2: Organizational Requirements
B. Affiliated Covered Entities	
(1) Requirements for Designation of an Affiliated Covered Entity	Section 2: Organizational Requirements
(2) Safeguard Requirements	Section 2: Organizational Requirements
(3) Retention Period	Section 2: Organizational Requirements

III. Security Standards (45 CFR 164.306)

Please refer to introductory section of manual

IV. Administrative Safeguards (45 CFR 164.308)

A. Security Management Process	
(1) Risk Analysis	Section 3: Security Management
(2) Risk Management	Section 3: Security Management
(3) Sanction Policy	Section 3: Security Management an Section 15: Sanctions
(4) Information System Activity Review	Section 3: Security Management and Section 5: Security of Information Systems
B. Assigned Security Responsibility	Section 3: Security Management
C. Workforce Security	
(1) Authorization and/or Supervision	Section 4: Workforce Security
(2) Workforce Clearance Procedure	Section 4: Workforce Security

Deleted: *7.02*

Deleted: *10*

Security Rule Implementation Specifications	Where is this Implementation Specification Addressed in the *HIPAA Security Policy and Procedure Manual*?
(3) Termination Procedures	Section 4: Workforce Security
D. Information Access Management	
(1) Isolating Health Care Clearinghouse Functions	*Not Applicable*
(2) Access Authorization	Section 5: Security of Information Systems
(3) Access Establishment and Modification	Section 5: Security of Information Systems
E. Security Awareness and Training	
(1) Security Reminders	Section 6: Security Training and Awareness
(2) Protection from Malicious Software	Section 5: Security of Information Systems
(3) Log-in Monitoring	Section 5: Security of Information Systems
(4) Password Management	Section 5: Security of Information Systems
F. Security Incident Procedures	
(1) Response and Reporting	Section 7: Security Incidents
G. Contingency Plan	
(1) Data Backup Plan	Section 8: Contingency Plan
(2) Disaster Recovery Plan	Section 8: Contingency Plan
(3) Emergency Mode Operation Plan	Section 8: Contingency Plan
(4) Testing and Revision Procedure	Section 8: Contingency Plan
(5) Applications and Data Criticality Analysis	Section 8: Contingency Plan
H. Evaluation	Section 3: Security Management
I. Business Associate Contracts and Other Arrangements	Section 9: Business Associate Contracts and Other Arrangements

V. Physical Safeguards (45 CFR 164.310)

A. Facility Access Controls	
(1) Contingency Operations	Section 10: Facility Access Controls and Section 8: Contingency Plan
(2) Facility Security Plan	Section 10: Facility Access Controls
(3) Access Control and Validation Procedures	Section 10: Facility Access Controls
(4) Maintenance Records	Section 10: Facility Access Controls

Deleted: *7.02*

Deleted: *10*

Security Rule Implementation Specifications	**Where is this Implementation Specification Addressed in the *HIPAA Security Policy and Procedure Manual*?**
B. Workstation Use	Section 11: Workstation Use and Security
C. Workstation Security	Section 11: Workstation Use and Security
D. Device and Media Controls	
(1) Disposal	Section 12: Device and Media Controls
(2) Media Re-Use	Section 12: Device and Media Controls
(3) Accountability	Section 12: Device and Media Controls
(4) Data Backup and Storage	Section 12: Device and Media Controls And Section 8: Contingency Plan

VI. Technical Safeguards (45 CFR 164.312)

A. Access Control	Section 13: Technical Controls
(1) Unique User Identification	Section 13: Technical Controls
(2) Emergency Access Procedures	Section 13: Technical Controls
(3) Automatic Logoff	Section 13: Technical Controls
(4) Encryption and Decryption	Section 13: Technical Controls
B. Audit Controls	Section 13: Technical Controls
C. Integrity	Section 13: Technical Controls
D. Person or Entity Authentication	Section 13: Technical Controls
E. Transmission Security	Section 13: Technical Controls
(1) Integrity Controls	Section 13: Technical Controls
(2) Encryption	Section 13: Technical Controls

VII. Organizational Requirements (45 CFR 164.314)

A. Business Associate Contracts or Other Arrangements	Section 9: Business Associate Contracts and Other Arrangements
(1) Business Associate Contracts	Section 9: Business Associate Contracts and Other Arrangements
(2) Other Arrangements	Section 9: Business Associate Contracts and Other Arrangements
B. Requirements for Group Health Plans	Not Applicable

Deleted: *7.02*

Deleted: *10*

Security Rule Implementation Specifications	Where is this Implementation Specification Addressed in the *HIPAA Security Policy and Procedure Manual*?
VIII. Policies and Procedures and Documentation Requirements (45 CFR 164.316)	
A. Policies and Procedures	OMPP Manual
B. Documentation	Section 14: Documentation Requirements
(1) Time Limit	Section 14: Documentation Requirements
(2) Availability	Section 14: Documentation Requirements
(3) Updates	Section 14: Documentation Requirements

Deleted: *7.02*

Deleted: *10*

Appendix B: Privacy/Security Incident Form

Please click on the following link to access the Privacy/Security Incident Form:

PDF

Incident Form

Deleted: *7.02*

Deleted: *10*

Appendix C:Facility Modification Form

Please click on the following link to access the Facility Modification Form:

Facility Modification Form

Deleted: *7.02*

Deleted: *10*

Appendix D: Notification of Transferred Equipment and/or Furniture SF44129

Please click on the following link to access State Form 44129 (Notification of Transferred Equipment and/or Furniture):

SF44129

Deleted: *7.02*

Deleted: *10*

Exhibit C

ORIGINAL REQUEST

Request for Bulk Data/Compiled Information

STATE OF INDIANA
IN THE _________________ COURT
CASE NUMBER __________

REQUEST FOR RELEASE OF BULK DATA/COMPILED INFORMATION (NOT EXCLUDED FROM PUBLIC ACCESS)

To the Executive Director of State Court Administration:

Pursuant to Administrative Rule 9(F) (3) this request for release of bulk data/compiled information that does not contain information excluded from public assess pursuant to Administrative Rule 9(G) or (H) is submitted:

I. **Identity of Applicant:** Indiana Family and Social Services Administration

Office of Medicaid Policy and Planning

Address:
402 W. Washington Street, W-374 MS 07
Indianapolis, IN 46204-2739

Telephone: (317) 232-2121

E-Mail: Mike.Staresnick@fssa.in.gov

II. **Identification of Bulk Data/Compiled Information sought:**

Case records including litigant /party indexes, listings of new case filings, including party names, chronological case summaries of cases and calendars or dockets of court proceedings compiled by Doxpop, LLC and by individual counties with electronic access to this information for Supervised Estates, Unsupervised Estates, Trust, and Guardianships.

III. **Identification of Court(s) Exercising Jurisdiction Over Records**

County Circuit, Superior, and Probate Courts.

IV. **Purpose of Request:**

The purpose of the request is to enhance the efficiency and effectiveness of the Office of Medicaid Policy and Planning in fulfilling its statutory responsibilities under 42 U.S.C. 1396 et. seq.

and I.C. 12-15-1, I.C. 12-15-2, I.C. 12-15-8.5 and I.C. 12-15-9. The release is consistent with Administrative Rule 9. Resources are available to prepare the information. The request is an appropriate use of public resources in that the requested information will be used to fulfill public purposes.

V. Attach a copy of each permission from a Court or County to obtain bulk distribution of Data or Compiled Information that has already been issued.

See Appendix A.

VI. Attach a copy of each Agreement Applicant has entered into with each Court or County listed in Section III to provide public access or to obtain bulk distribution of Data or Compiled Information.

See Appendix B.

VII. Identify the frequency with which bulk Data and Compiled Information is being requested to be transferred to applicant by each Court or county listed in Section III.

Monthly

VIII. Describe the resources available to prepare the information.

The Indiana Family and Social Services Administration's Office of Information Technology, and Data Warehouse are utilized to prepare information in support of the agency's needs. Currently the agency is developing data matches with Doxpop, LLC for those counties making information available through Doxpop, LLC.

IX. Describe how fulfilling the request is an appropriate use of public resources.

The request is to enhance the efficiency and effectiveness of the Office of Medicaid Policy and Planning in fulfilling its statutory responsibilities under 42 U.S.C. 1396 et seq and I.C. 12-15-1, I.C. 12-15-2, I.C. 12-15-8.5 and I.C. 12-15-9. The agency is charged with responsibility to recovery medical assistance payments made on behalf of Medicaid recipients received after age fifty-five (55) from the individual's estate. All funds recovered are returned to the Medicaid program to assist others in need.

X. **Applicant is (is not willing to pay the reasonable cost of responding to this request. If not why?**

The Office of Medicaid Policy and Planning is willing to pay the reasonable cost of responding to the request.

XI. **Does this Request include a request for permission to transfer the bulk Data and Compiled Information to a third party?**

No. The information will only be accessible to limited number of staff within the Office of Medicaid Policy and Planning. A copy of the HIPPA Privacy Policy is attached as Appendix C.

By signing this request, I represent that I am authorized to do so on behalf of Applicant.

Michael J Staresnick
Signature

Michael J. Staresnick
Printed Name

Estate Recovery Manager
Title

~~April 10, 2008~~ February 10, 2009
Date

Exhibit D

APPROVAL LETTER

STATE of INDIANA

DIVISION OF
STATE COURT ADMINISTRATION

RANDALL T. SHEPARD, CHIEF JUSTICE

LILIA G. JUDSON, EXECUTIVE DIRECTOR

SUPREME COURT

115 WEST WASHINGTON STREET SUITE 1080
INDIANAPOLIS, IN 46204-3466
(317) 232-2542
FAX (317) 233-6586
www.IN.gov/judiciary

June 6, 2007

Michael J. Staresnick, M.P.A.
Estate Recovery Manager
Family & Social Services Administration
Office of Medicaid Policy & Planning
MS07, 402 W. Washington St., Rm W382
Indianapolis, IN 46204-2739

Dear Mr. Staresnick:

Enclosed is an Amended Bulk Data User Agreement for your review and execution. The Division of State Court Administration requires this agreement to be fully executed by both the requestor and the Executive Director of the Division of State Court Administration prior to giving final approval for obtaining bulk data from Indiana courts. Included in the agreement are several attachments, which need to be provided by the Requestor. Once the Division reviews the signed Bulk Data User Agreement, you will receive a notification that either it has been approved or the Division needs more information. If approved, you are then able to contact the relevant individual courts or clerk's offices to make arrangements for bulk data transfers. Additional costs, scheduling, and other considerations may be necessary as you work with individual courts or clerk's offices.

Execution of the Bulk Data User Agreement does not create an obligation on the part of individual courts or clerk's offices to provide bulk data. Rather, execution of this agreement merely permits requestors to approach individual courts or clerk's offices and make arrangements to receive bulk data **if** that court or clerk's office is capable of transferring bulk data and has sufficient resources to do so. All relevant courts and clerk's offices will receive notification of approved bulk data requestors from the Division of State Court Administration.

Please note that the User Agreement has been changed and requires additional documentation and attachments. The Agreement will expire, subject to renewal, on January 31, 2008.

Follow-up phone calls regarding this correspondence or to check on the status of user agreement approvals are not necessary. However, should you have additional questions about this process or requirements, please contact me at (317) 232-2542.

Sincerely,

Kristin Donnelly Miller

Kristin Donnelly-Miller, Esq.

Enclosure

Exhibit E

DISTRIBUTION RECEIPT FORMS